방화벽 환경에서의 VNC 기반 역방향 원격제어 방법 및 시스템 구현

조명진, 김선욱
고려대학교 전자전기공학과
linux@korea.ac.kr
seon@korea.ac.kr

A Method of VNC-based Reverse Remote Control and System Development for Firewall Environment

Myeongjin Cho, Seon Wook Kim
School of Electrical Engineering, Korea University

요 약

최근 원격 제어 시스템은 언제 어디서나 인터넷에 연결되어 있으면 회사나 학교 등 원격지에 위치한 컴퓨터에 접속하여 작업을 수행할 수 있게 해준다. 원격지의 컴퓨터를 어디서나 사용할 수 있게끔 해주기 때문에 재택 근무 등을 이유로 집과 학교와 같은 장소에서 동일한 컴퓨팅 환경을 구성해야 하는 불편함을 없애준다. 그러나 최근 다양한 네트워크 공격과 해킹의 시도로 인해서 회사나 학교에서는 방화벽을 사용하여 외부로부터의 허용 되지 않은 패킷을 차단하기 때문에 이러한 이점을 지닌 원격제어 시스템을 사용하지 못하는 경우가 많다. 이에 외부에서 방화벽 내의 시스템을 접근할 수 있도록 역방향 원격제어 방법을 제안하고 오픈소스인 VNC를 기반으로 원격제어 시스템을 개발하였다.

1. 서론

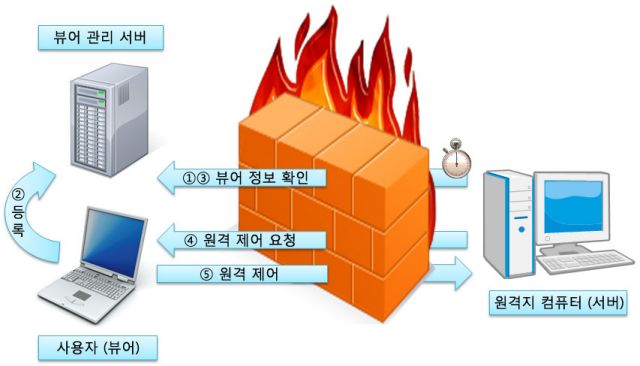
최근 원격제어 시스템은 인터넷에 연결되어 있는 곳이면 어디서나 장소에 구애받지 않고 원격지의 컴퓨터를 안전하고 빠르게 사용할 수 있게 해준다. 그래서 원격지의 서버를 관리하거나 출장 중 혹은 재택 근무를 하게 될 경우 원격제어 시스템을 이용하여 원격지의 컴퓨터를 쉽게 사용할 수 있다. 또한 최근에는 컴퓨터 기반 서비스의 A/S를 위해서 상담원이 고객 컴퓨터에 접속하여 문제를 해결해 주는 등 다양한 형태로 응용되고 있다.

그러나 최근 크게 문제가 되고 있는 DDoS(Distributed Denial of Service Attack)[1]나 포트 스캐닝[2] 등을 이용한 다양한 해킹 공격으로 인해서 대부분의 회사나 학교는 방화벽을 구축하여 인트라넷의 보안을 유지하고 있다. 이렇게 방화벽이 구축되어 있는 환경에서는 원격지에서 내부 네트워크로 접속하는 패킷 중 허용되지 않은 패킷을 필터링하기 때문에 원격제어 시스템을 사용할 수 없는 경우가 대부분이다. 이러한 문제를 해결하고자 방화벽이 신뢰하는 HTTP 포트(80)와 같은 열린 포트를 사용하거나 원격지의 컴퓨터에 웹 서버를 설치하여 웹 브라우저나 뷰어를 이용하는 형태의 원격 제어 방식을 사용하고 있다.

하지만 최근 웹 해킹을 통해서 시스템 권한을 획득하여 내부 네트워크의 다른 시스템을 공격하는 해킹이 많아지면서 웹 서버가 아닌 일반 사용자의 컴퓨터에서는 HTTP 포트를 허용하지 않는 경우가 많아지고 있다. 이처럼 허용되는 포트가 전혀 없는 방화벽 환경에서는 위와 같은 서비스는 무용지물이 되고 만다. 이러한 방화벽 환경에서의 문제를 해결하고자 일반적으로 뷰어가 원격제어 서버에 접속하는 방식을 탈피하여 서버가 뷰어에 접속하는 역방향 원격제어 시스템을 개발하였다.

2. 역방향 원격제어 시스템

기존의 역방향 원격제어 시스템은 상담원과 고객의 관계에서 주로 사용하였기 때문에 서버가 뷰어에 원격제어를 요청하는 방식을 사용하고 있다. 그러나 서버에서 뷰어로 요청해야 하는 방식 때문에 서버 관리나 재택 근무와 같은 상황에서는 사용이 불가능하다. 이에 다음과 같은 구조의 역방향 원격제어 시스템을 제안한다.



(그림 1) 역방향 원격제어 시스템

그림 1에 명시된 바와 같이 제안하는 역방향 원격제어 시스템은 서버, 뷰어 그리고 뷰어 관리 서버로 구성되어 있다. 일반적인 원격제어 시스템과 같이 서버와 뷰어는 원격제어의 대상자와 사용자이며 여기에 뷰어가 원격제어를 하기 위해 준비상태에 있음을 알려주는 뷰어 관리 서버가 추가되었다. 서버는 설정에 따라 주기적으로 뷰어 관리 서버에서 접속하여 준비된 뷰어가 있는지를 확인한다. 만약 준비된 뷰어가 없다면 다음 주기까지 대기상태로 있게 된다. 뷰어는 원격제어를 위해 자신의 IP 주소와 포트 정보를 뷰어 관리 서버에 기록하고 Listening 모드로 전환하여 서버로부터의 원격제어 요청을 기다린다. 이때 서버는 뷰어가 준비되어 있음을 확인하고 IP 주소와 포트 정보를 통해 역방향으로 뷰어에 원격제어를 요청하게 된다. 이에 뷰어는 서버로부터의 원격제어 요청을 받아들여 원격제어를 시작한다.

여기서 뷰어 관리 서버는 웹 서버이며 다수의 사용자를 위해서 원격제어 시스템을 위한 별도의 서비스를 제공할 수 있다. 또한 사용자가 웹 서버의 계정을 보유한 경우 단순히 다음 형태의 XML 파일을 웹 서버에 업로드 하는 것으로 대체할 수 있으며 심지어 게시판에 XML과 같은 형식의 글을 올리는 것으로도 대체가 가능하다.

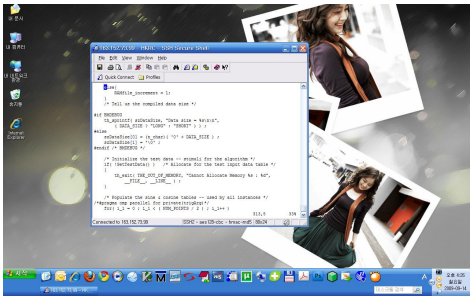
예제 1) 뷰어 등록 XML 예제

```
<VIEWER>
<IP>211.212.4.107</IP>
<PORT>5500</PORT>
<ENABLE>1</ENABLE>
</VIEWER>
```

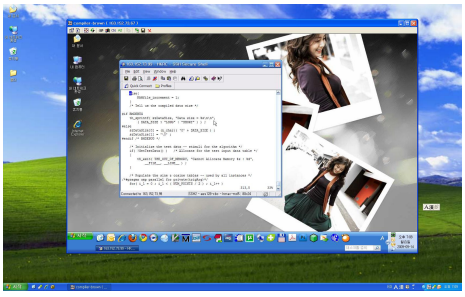
뷰어에 대한 정보는 예제 1에서 볼 수 있듯이 뷰어가 존재하는 시스템의 IP 주소와 원격제어 포트 번호로 구성되어 있다. 포트 번호는 기본적으로 5500번을 사용한다. 마지막으로 ENABLE 값이 0이라는 것은 뷰어가 비활성화되어 있는 것을 뜻하며 이 경우 서버는 뷰어로 원격제어를 요청하지 않는다.

3. 구현 결과

역방향 원격제어 시스템은 오픈소스 원격제어 프로그램인 VNC(Virtual Network Computing)를 바탕으로 제작되었다. 뷰어와 서버는 UltraVNC 1.0.2[3] 버전을 수정하여 개발하였으며 뷰어는 Listening 모드를 지원하는 다른 VNC 뷰어와 호환이 가능하다. 또한 뷰어 관리 서버는 방화벽 외부의 웹 서버에 XML을 업로드하는 방식을 사용하였다. 여기서 뷰어 관리 서버가 반드시 방화벽 외부른 V어야 하는 것은 아니며 방화벽 내부른 V어도 서비스른 전혀 문제가 되지 않는다. 그리고 방화벽 테스트 환경은 고려대학교 네트워크를 사용하였다. 고려대학교는 기본적으로 외부로부터의 모든 포트를 차단하고 복잡한 승인 절차를 통해서 허용된 IP 주소에 대해서만 HTTP 포트를 개방해주며 해당 포트는 웹 서비스만을 허용하도록 제한하고 있다. 뷰어는 고려대학교 네트워크 외부의 지역 ISP(Internet Service Provider)를 이용하였다.



(그림 2) 원격지 컴퓨터 화면



(그림 3) 뷰어를 통한 원격 제어 화면

그림 2는 원격지 컴퓨터의 화면을 보여주고 있다. 예제 1과 같이 뷰어의 정보를 서버에서 설정한 뷰어 관리 서버로 등록하게 되면 서버가 뷰어 정보를 확인하는 대로 그림 3과 같이 원격제어가 시작된다.

4. 결론

외부로부터의 접속에 대해서 모든 포트를 차단하는 방화벽 환경에서는 원격제어 시스템은 때론 무용지물이 되어 버린다. 이에 뷰어 관리 서버를 이용하여 역방향으로 원격제어를 요청함으로써 이러한 방화벽으로 인한 제한을 해결할 수 있었다. 또한 뷰어 관리 서버가 매우 단순한 방식이므로 역방향 원격제어 시스템을 구성하기 위해 별도의 큰 비용을 추가할 필요가 없다. 추후 인증 절차를 추가하고 패킷을 암호화한다면 보다 안전하고 신뢰성 있는 서비스를 제공할 수 있을 것이다.

참고문헌

[1] Lau F., Rubin S.H., Smith M.H, Trajkovic L., "Distributed denial of service attacks," Systems, Man, and Cybernetics, 2000 IEEE International Conference on , vol.3, no., pp.2275-2280 vol.3, 2000

[2] M. de Vivo, E. Carrasco, G. Isern and G. de Vivo, “A Review of Port Scanning Techniques,” Computer Communication Review, 29(2), April 1999.

[3] UltraVNC, http://www.ultravnc.com/